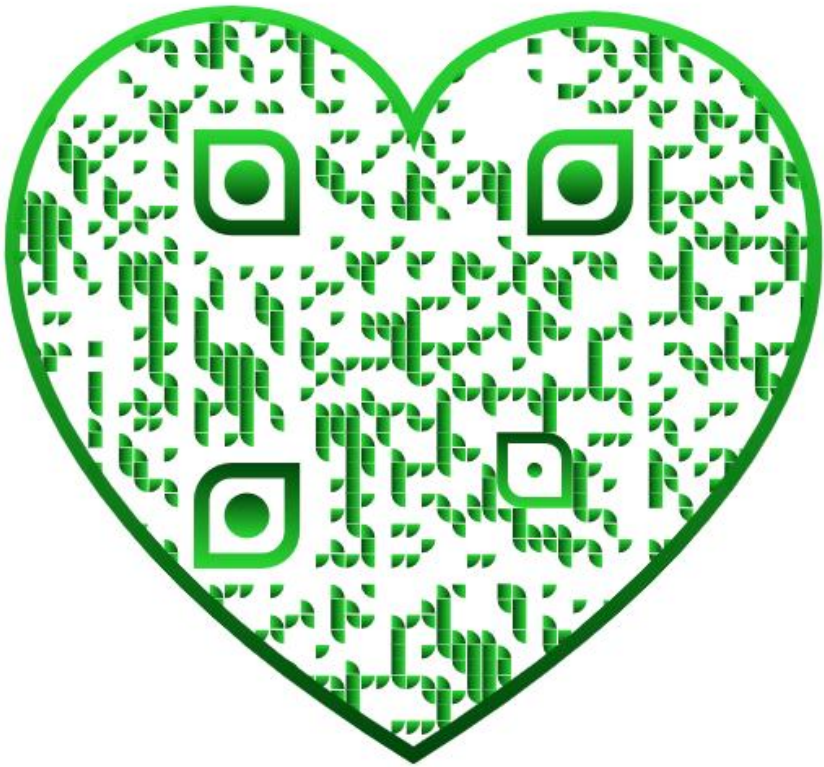
HACKING

LE GUIDE COMPLET DU DÉBUTANT ÀORDINATEUR PIRATAGE ET TESTS PÉNÉTRATION

MILES PRICE



HACKING

LE GUIDE COMPLET DU DÉBUTANT ÀORDINATEUR PIRATAGE ET TESTS PÉNÉTRATION

MILES PRICE

Hacking

Le Guide Complet du Débutant àordinateur Piratage et Tests Pénétration

Miles Price

Tableaudes matières

Introduction
Chapitre 1: Il estmonde d'Hacker!
Chapitre 2:Test
Chapitre 3pénétration:Méthodologie de The
Chapitre 4Hacker:Obteniraccès physique
Chapitre 5:ingénierie sociale
Chapitre 6: Piratagemotspasse
Chapitre 7: Réseau sans fil Attacks
Chapitre 8: Piratageun Smartphone
Chapitre 9: Piratage Conseils pourdu débutant
Conclusion
ressources

Présentation

Cybercriminalité est la plus grande menace que chaque organisation sur la planète fait face aujourd'hui! Et ce n'est pas seulement les organisations qui sont vulnérables.gens sont trop à risque d'êtrecible parpirates.

Dans ce livrenous voulons vous montrer l'importance de rester audessus de cette menace en apprenant comment pirater. Il est vrai quepirates ont reçu une mauvaise réputationfil des ans, principalementraison de reportages des médias biaisés, touspirates ontintentions criminelles.

Ce livre est destiné à servir de guide pédagogique pourgens qui sont intéressés à apprendre des outils de piratage simples,astuces ettechniques afin de vous protéger et protéger vos réseaux informatiques.

Il doit être utilisé pourpiratage éthique et nonactivités malveillantes. Si vous avez déjà été curieuxsujetpiratage et ont voulu apprendre l'art du hack, alors vous avez trouvé le bon livre.

Nous vivons dans un monde où tout est interconnecté.retour dans la journée, nous nous sommes appuyés sur les organisations gouvernementales etgrands pour fournir suffisammentsécurité pour nos données personnelles. Ce n'est plus possible dans un monde où les agences de sécurité euxmêmes sont les principales cibles des pirates.

En fait, dansplupartcas, la plus grande menace cybernétique viendra de votre propre gouvernement!

Donc que fais-tu? Asseyezvous et croisez les doigts,espérant que votre parefeu et antivirus sera suffisant pour vous protéger? Que vousvouliez ou non, vous devrez apprendre à pirater si vous allez avoir une chance de garder vos propres systèmes de cybersécurité.

En comprenant commentpirates malveillants font ce qu'ils font, vous serez en mesure de détecter etprévenir les menaces potentielles à un système informatique ouréseau. Ce livre vous aiderafaire.

Nous commençons par un aperçu général de l'état desécurité mondiale cybernétique. Vous apprendrez à faire une distinction entre les différents types de pirates làbas, leurs motivations et les compétences que vous avez besoin pour commencerpiratage toutsuite.

Nous couvrirons également comment effectuertests de pénétration pour vérifier touteslacunes potentielles dans un réseau. Chaque

réseau, quellesoit la sécurité, a une sorte de faiblesse. Vous apprendrez ce qui se passe dansciblage,numérisation etanalyseune cible, et comment accéder à un système.

Il existe différentes façons de piratageun système informatique. Nous prenons un regard en profondeur sur certaines des tactiques haut qui utilisentpirates malveillants pour lancerattaques sur leurs cibles. Enfin, que pouvezvous faire pour restersécurité comme un hacker? Lisezpropostout cela et plus ici.

Ce livre a été traduit par un logiciel automatisé pour atteindre un public plus large. S'il vous plaît ignorer une traduction erronée.

Je vous souhaite le livre!

© Copyright 2017 - Tous droits réservés.

Le contenu de ce livre ne peut être reproduite, dupliqués ou transmis sans autorisation écrite directe de l'auteur.

En aucun cas, aucune responsabilité légale oublâme lieu contre l'éditeur pour une réparation,dommages oupertes financièresraison des informations présentes,soit directement ou indirectement.

Mentions légales:

Ce livre est protégécopyright. Ceci est seulement pourusage personnel. Vous ne pouvez pas modifier, distribuer, vendre, utiliser, devis ou paraphraser tout ou partie du contenu de ce livre sans le consentement de l'auteur.

Avertissement Avis:

S'il vous plaît noter les informations contenues dans ce document sont àfins éducatives etdivertissement seulement. Touseffort ont été faits pour fournirexactes, à jour et complètes fiables. Aucune garantie de quelque nature qu'elle soit explicite ou implicite.lecteurs reconnaissent que l'auteur ne se livre pas dans le rendu des conseils juridiques, financiers, médicaux ou professionnels. Le contenu de ce livre a été dérivé de sources diverses. S'il vous plaît consulter un professionnel agréé avantessayer des techniques décrites dans ce livre.

En lisant ce document, le lecteur accepte queen aucun cas, l'auteur est responsable des pertes, directes ou indirectes, qui sont engagés à la suite de l'utilisation deinformation contenue dansprésent document, y compris, mais sans s'y limiter, -errors , omissions ou inexactitudes.

Chapitre 1: Il estmonde d'Hacker!

Les jours de repos sachant facile que vos informations privées estabri des regards indiscrets sont plus! Le mondenous vivons actuellement n'est plus ce qu'il. La cybercriminalité est une menace réelle, dangereuse et persistante que chaque organisation etbesoins individuels à prendresérieux.ce momentnous vivons à l'ère numérique et dans un village global. Avec tout et toutmonde interconnecté à une telle échellemasse, il est sûr de dire que c'est le monde d'un pirate informatique.

Le nouveau président américain luimême, Donald Trump, a déclaré quevol de cyber est le crimeplus rapideplusplus en Amérique. Ce n'est pas son opinion personnelle. La communauté desécurité informatiqueaccord aussi.

Vous ne me croyez pas? Voyons quelques statistiques.

1. Saviezvous que les dommages causés parcybercriminalité en 2016coûté 3 billions $, et devrait atteindre 6 billions $annéeici l'an 2021?
2. Saviezvous queorganisations partout aux ÉtatsUnisdépensé un total de 80 milliards $ surproduits et services pour se protéger contre la cybercriminalité? Ce chiffre devrait dépasser 1 billion $ en 2017.
3. Saviezvous qu'il n'y a pratiquement aucune chance de chômage si vous travaillez dans l'industrie desécurité informatiquece moment?analystes ont conclu qu'il ya une pénurie extrême de talents decybersécurité partout dans le monde, le taux de chômage desécurité informatique tomber à zérocentpartir de 2016!
4. pirates sont maintenantaprèssang, passilicium. Selon Microsoft, il y aura 4 milliardspersonnesligneici l'an 2020, ethumains, pasordinateurs, sont maintenant la principale cible des pirates.
5. Saviezvous que le pirate moyen estmesure de restersommeil dans votre réseau pour une moyenne de 200 jours sans être détecté?

Ces statistiques ne sont pas destinées à vous faire peur. Ils sont destinés à ouvrir les yeux sur ce qui se passe partout dans le monde. Si vous regardez et lisez les nouvelles, vous devez comprendre l'ampleurce problème prendra l'avenir.

Hacking Défini

Ce qui vient àvotre esprit quand vous entendez le mot « piratage? » Imaginez-vous un personnagecapuchon penché sur un ordinateuressayant d'obteniraccès illégal à un réseau pour volerdonnées? Ou peutêtrepeu intello geeky avec rien à faire toutejournéemais envoyer des programmes cryptés pour infecterréseaux etsystèmes?

Quelles que soientimages peuvent avoir sauté dans votre tête, le fait est queplupartgens croient que touspirates ontintention de volerinformations ou espionnergens. La majorité des gens pensent que touspirates sontcriminels etpiratage est mauvais. Cela peut être ce qui est dépeint dansfilms et émissions de télévision, mais il est tout simplement pas le cas.

Hacking peut être définie comme une tentative de résoudre un problème ouaméliorer une application par matériel ou logiciel réingénierie. Enautres termes, si vous avez un problème avec votre ordinateur et ne parvenez pas àrésoudreutilisanttechniques classiques, alors vous pouvez être forcé d'utilisertechnologie est disponiblemais d'une manière nouvelle. Si vous regardez l'histoire defaçon dontcommencépiratage, tout a commencé avec l'intention de résoudre un problèmeutilisantmoyens créatifs.

Les premiers enregistrés « pirates » étaient un groupe de geeksMIT qui ont utiliséancien équipement téléphonique pour contrôler leur modèletrains retour dans les années 1950. Ces garslà étaient tellement en forme quemodèle qu'ils ont pris l'équipement téléphonique qu'ils avaient reçu comme un don et conçus pour que plusieurs opérateurs puissent contrôler la voie ferrée en composant simplement le téléphone.

Certains de ces garslàmême allés plus loin etcommencémodifier les programmes informatiques récemment misplace surcampus. Leur objectif était de personnaliser les programmes pour usage spécial etrendre mieux. Ils ont simplement utilisé ce qu'ils avaientdisposition de faire preuvecréativité,inventer une nouvelle façon de faire quelque chose, et résoudreproblèmes.

C'est ce que hacking est sur. Aujourd'hui,piratage peut représenter une violation decybersécurité,systèmes dommageables etaccès illégal, mais ce n'est pas toute l'histoire.

Alorscomment distinguez-vous les bons gars des criminels?

La psychologie de Hacking

Pour arrêter un hacker, vous devezabord comprendre ce qui les motive. Dans la communautépiratage, il y a plusieurs niveaux de compétences diverses et complexes et motivations. Il est important que vous compreniez les différents types de pirates informatiques afin que vous puissiez êtremesure de prédire leurs tentatives etcomprendre leur mentalité. Mêmetant que débutant qui apprend comment pirater un système, vous ne voulez pas vous laisser vulnérable à une contreattaque.

Catégories de pirates

Les plus gros erreurgens font estmettre touspirates dans le même groupe que si elles ont un seul but. Cela est souvent ce que les médias fait, et le public est tombé pour ce mensonge. Vous ne pouvez pas tenter de classer un pirate sans savoir pourquoi ils ont joué le hack et quelsleurs objectifs étaient. La communautépiratage est quelque peu divisée surfaçon de nommerdifférents types de pirates, mais en général, ce sont les catégories queplupartgensaccord sur:

- **White Hats** - également connu comme «*hackers éthiques*», ces pirates opèrent dans la loi. Ils collent à l'éthique du hacker, qui stipule qu'un pirate doit « ne pas nuire ». Ils travaillent aussi commeexperts desécurité cybernétique et sont embauchés pour détectervulnérabilités potentielles dans un système ouréseau, et les corriger. Ce type de pirate informatique travaille avecéditeurs de logiciels pour patcher une vulnérabilité dans leur logiciel. Chapeaux blancs font généralement ce qu'ils fonttant que service public. Leur but est de sensibiliserpublic aux menaces làbas afin quegens sachent comment un système est vulnérable. Cependant, ils ne publient publiquement ces données jusqu'à ce que le fournisseur du logiciel a fait euxmêmes.

- **Black Hats** - Ce type de pirate est souvent convaincu qu'ils sonttrainfaire un service public, mais en réalité, leur principale motivation estpouvoir etargent. Ils ont tendance à pénétrerréseaux afin qu'ils puissent voler ouendommager les données. Ils sont animés parhaine oucolère malveillante contre une organisation oupays. Il est intéressant de noter qu'ils ont obtenu leur nom du fait queméchants dansplupartfilms occidentaux cowboy portaientchapeaux noirs.

- **Gris Chapeaux** - Ce terme a été initialement présenté par un groupepiratagevieille école très célèbre qui ne voulait pas être associé avecchapeaux noirs ne sont pas encore désireux de être stigmatisés comme testeurs de sécuritéentreprise. Chapeaux gris

peuvent être décrits commepirates qui ont utilisé comme Black Hatsmais ont reformé et travaillent maintenant commeexperts en sécurité informatique. Ils sont parfois définis commepirates qui consultent ainsi queaccès illégal aux gains réseaux.

Classes de pirates

Il y aclasses spécifiques qui relèvent des catégories de pirate Chapeau noir et blanc mentionnés cidessus. Ceuxci comprennent:

- **Elite** - Ce sont les gourous du mondepiratage. Ils ont les compétences etconnaissancespersonne n'aautre. Mais ce qui les rend extrêmement rare est leur éthique etintégrité. Ils agissent souvent comme White Hats qui connaissentinfrastructure réseau et possèdent les connaissances de programmation pour écrire leurs propres outils. Ils ne sont pas motivées parintentions criminelles et sont plusintention dedétectionproblèmescodage oufailles de sécurité etinformeradministrateurs système. Vous ne pouvez devenir un hackerélite en effectuant un hack bien connu ou exploiter oumaintenirlongévitétant que pirate.

- **Cyberterroristes** - Cette classe de pirate va audelà écraser un réseauutilisant un déni de service (DoS). Ils se développent et aiment le fait qu'ils peuventcacher derrière le voile du Web comme ils partagentinformation entre eux. Ils sont capables de cacherdonnées chiffrées dansvuesorte que seul un homme cybercriminel peuttrouver.gouvernements partout dans le monde ont tendance à embaucher ces types de pirates pour faire leur sale affaire, allant deespionnage simple à la cyberguerre.

- **Script Kiddies** - Personne est aussi décrié ou ridiculisé comme script kiddie. Cette classe de pirate est jeune, inexpérimenté, et non qualifiée pour créer leurs propres outils exploiter. Ils utilisentoutils fabriqués parpiratesélite, et ne peuvent piratersystèmes queautres ont relevévulnérabilités. Ils piraterpluparttemps pourplaisir et sont ceux dontexploits sont souvent mentionnés dans les médias. Leurs principales réalisations sont généralementattaques DoS et page web défiguration.

- **Hacktivistes** - Ceci est une combinaison d'un hacker et activiste. Ils portentprogrammes politiques, sociaux ou religieux et peut être très tenace. Ils défigurentsites Web et effectuerattaques DoS à faire pression surgouvernements ouorganisations qu'ils considèrent causentdommages à un groupe particulier desociété.

- **Employéscolère** - Ce sontgens qui ontconnaissancesintérieur d'une organisation etutiliser leur accès à recueillirinformation pour euxmêmes ouautres. Ils sont considérés comme extrêmement dangereuxmême si le public est rarement en entendre parler. Ces pirates sont généralement calme et timidemais ontpersonnalités narcissiques. Ils tournent sur leurs employeurs chaque fois qu'ils croient qu'ils ne sont pas reconnus pour leur travail.

- **auteurs de virus** - Ce sontgens qui profitent de toutesfaiblesses qu'un pirate informatique a exposés, et vont à écrirecode pour exploiter ces vulnérabilités.

Compétences requises pour Hacking

tant que débutant, il y a des compétencesbase que vous devez développer si vous êtes à progresser dans le monde du piratage informatique. Ceuxci comprennent:

1. **Outils informatiques maîtrisés** - Vous devez êtreinformés dansutilisation des ordinateurs et êtremesure de comprendreinstructions écrites. Naviguer sur Internet sans but ne compte pas. Pouvezvous utiliser le module de commande Windows? Ces compétencesbase sont essentielles pour chaque piratevaleur leur sel.
2. **bonne connaissance de Linux OS** - Linux vous permet de personnaliser vos programmes,qui explique pourquoipirates préfèrent sur Mac et Windows.
3. **Compétences de base de données** - Apprendre à utilisersystèmes de gestion de bases de données comme Oracle et MySQL vous aidercomprendre comment pénétrerbasesdonnées.
4. **Compétencesréseau** -tant que pirate informatique qui sera engagé dans beaucoup d'activitéligne, vous devez savoir surconcepts telssousréseaux, DNS,ports,motspasse WPS, et ainsisuite.
5. **Compétences de script** - Vous ne pouvez pas savoir comment le codece moment, mais tôt ou tardvous devrez apprendre. Chaque piratebesoin d'avoir leurs propres outils de piratage plutôt quedépendre de ce queautres ont créé.se fondant suroutils faites parautres pirates laisse votre système vulnérable àexploitation. Preneztemps d'apprendre quelques langages de script tels que Ruby on Rails ou Python.
6. **Compétences en ingénierie inverse** -un des moyens les plus efficaces pour développer un outil de piratage informatique est de prendre un existant, démonter, et trouver un moyen de faire mieux. Ces compétences sont inestimables pour un pirate informatique.
7. **utilisation de logiciels de virtualisation** - Ce type de logiciel permet de testertoute sécurité votre hack sur votre ordinateur avantlâcher sur quelqu'unautre. Un bon exemple est VMWare Workstation.

Qu'estcemotive un Hacker?

Il futqueopérationspiratage ont été menées par un collège oucachette pour adolescents du secondaire au soussol de leurs parents.nos jours,cyberattaques sont plus sophistiquées etgrande échelle. Pourtantdépit du fait que la cybercriminalité a progressé à un rythme alarmant avecmeilleure technologie, les motivations du hacker d'aujourd'hui ne diffère guère de celle de la génération précédente.

Donc ce qui motive un cybercriminel à pirater un réseau ousystème? Il y a quatre raisons fondamentales:

1. **argent** -gain financier est le plus grand facteurmotivation deplupart des cyberattaques d'aujourd'hui. Vous avez entendu parler de pirates exploitantvulnérabilités du système des institutions financières et de partir avecnuméros de cartes de crédit, comptes de messagerie, motspasse, nomsutilisateur, etc Un hacker malveillant va vendre tout ce qu'ils peuvent trouver pour un prix. Certains chapeaux noirs même Organizations chantageaide ransomware.
2. **Agenda politique / Idéologique** - C'est là hacktivistes tombent sous. Ils attaquent les réseaux d'institutions gouvernementales,organisations etpersonnalitéspremier plan pour faire avancer leurs programmes idéologiques, politiques, sociaux ou scientifiques. Un groupe connu pour avoirtelles motivations sont anonymes.
3. **Divertissement** - La majorité des gris chapeaux ont tendance à exploiterréseaux pourplaisir oufierté. Ils cherchent un défi etviolationlois éthiques pour satisfaire leur curiosité. Cependant, ils ne sont pas malveillants et vont même informer l'administrateur réseau sur les vulnérabilités qu'ils trouvent.
4. **Cybersécurité** - White Hats généralement un système exploit de trouverfaiblesses afin qu'ils puissent les rendre plus sûres.organisations emploient souventpirates de travailler pour eux,vulnérabilités de patch, et créercodes de pratique pouremployés à suivre pour éviteratteintesla cyber.

Chapitre 2:intrusion tests

Testspénétration fait référence à l'essai d'un système cybernétique, réseau ouapplication pour détecterfaiblesses qui peuvent être exploitées par un pirate malveillant. Vous essentiellement essayez d'accéder à un système sans avoir de nomsutilisateur oumotspasse. L'objectif est de voir comment il est facile d'obtenirinformations confidentielles sur une organisation, puis augmenter la sécurité du système testé.

Alorsquelle est exactement la différence entre un test de pénétration et une attaque? permission!

Un pirate informatique qui effectue un test de pénétration sera donné l'autorisation par le propriétaire du système, qui sera ensuite attendre un rapport détaillé à la fin de tout.tanttesteur, on peut vous donner accès au niveau utilisateur pour vous permettre d'entrer dans le système.partirlà, vous devrez vous attendre à voir s'il est possible d'avoir accès àinformations confidentielles qu'un utilisateur ordinaire ne devrait jamais voir.

L'autre option est d'aller en aveugle. Dans une évaluation aveugle ou secrète, vous n'êtes pas donné des informationsexception du nom de l'organisation cliente. Le reste est à vous,qui est exactement commentpiratesplus malveillantsfonttoute façon. Le seul problème avec une évaluation secrète est que cela prendra plustemps qu'un un manifeste,augmente les chances de vous manquer une faille.

Vous pouvez être embauché pour trouver une seule faiblesse, mais dansplupartcas, vous serez appelé à continuerchercher pour trouver toutes les vulnérabilités potentielles dans un réseau. Une fois identifié, vous devrez trouvermoyens de fixationces trous. Ceci estraisonlaquelle vous devrez écrirenotes détaillées concernant votre procédure de test etrésultats.prisenotes permet au client de déterminer l'efficacité de votre travail et vérifier si les problèmesvous avez découverts sont bien fixés. Cependant, il est très peu probable que vous détecter tousdéfauts de sécurité unique outrou dans le système.

détectionvulnérabilités

Les mesures prises par un testeur de pénétration et un hacker malveillant sont généralement les mêmes. Dansplupartcas, un hacker malveillant se déplace lentementtravers un système afin d'éviterêtre détectés. Vous pouvez également suivre la même tactique pour voir à quel point efficace le système d'un client est à détectertelles attaques. Une fois cela fait, ces lacunes doivent être scellés.

La première étape est généralement reconnaissance. Vous essayez de recueillir autantinformations sur votre réseau cible que vous le pouvez. Ceci est normalement un processus passif qui consisteutiliserressources disponibles au public. Vous pouvez identifier les serveurs Web de l'organisation, OSil estcoursexécution, la version du logiciel, patchs ou modules serveur a permis,adresses IP, et dans certains cas, même le nom du serveur interne.

Lorsque vous avez rassemblé vos informations, il est alors temps devérifier. Ceci peut être réalisé en comparant les informations de réseau ousystème avecvulnérabilités connues recueillies. Une foisvous tester les vulnérabilités, vous saurez avec certitude si les informationsvous aviez recueillies sont exactes ou non.

Raisons pour effectuertestspénétration

1. Identifierfaiblesses quepirates malintentionné pourrait

Même que vous lisez ce livrece moment, il est possible qu'il y aitpirates malveillants lancementoutils etattaques de réseau pour tenter de pénétrervotre système. Ces attaques sont sans fin et vous ne pouvez pas prédire quand un système sera touché. Dansplupartcas, ces exploits sont bien connus et donc évitables. Le service informatique d'une organisation peut être désireux de savoir où sont les faiblessesseinleur réseau et comment un hacker malveillant peuttirer profit.tant que testeur de pénétration, vous devrez attaquer le système et fixer les trous avantquelqu'un avecmauvaises intentions trouve leur chemin. Un système peut être sécurisé aujourd'huimais demain il peut être victime d'une violation.

1. Justifier àgestion du besoin de ressources

Il y amoments où la haute direction ne voit pas seulement la nécessité d'allouer davantageressources financières verssécurité cybernétique. Dans ce cas,tests de pénétration est la meilleure façon pour l'équipe de sécurité de l'entreprise pour justifier leurs demandes de plusfonds. L'équipe desécurité informatique peut êtrecourant des vulnérabilitésmaisgestion résiste àappui changements apportés au système existant. En externalisant les tests à un consultant externe,gestion est plus susceptible de respecter les résultats obtenus.

1. Assurezque l'équipe de sécurité interne fait son travail

Le rapport de test de pénétration montrera si le ministère desécurité informatique est efficace dans son travail. Il peut déterminer s'il y a un écart entreconnaissances des vulnérabilités du système etmiseœuvre des mesures de sécurité.

1. formation du personnel du réseau

Imaginez si un pirate devait avoir accès au système d'une organisation sans le personnel mêmesavoir. En effectuant un test de pénétration, il est possible de découvrir à quel point vigilant votre sécurité et si le personnelbesoinformation supplémentaire. Il met égalementévidence l'efficacité des contremesures qui ont été mises en place en cas d'une cyberattaque.

1. Test des nouvelles technologies

Avantlancer un nouveau morceau detechnologie, par exemple, une nouvelle infrastructure sans fil, il est essentiel que le système est testé pourvulnérabilités. Cela va certainement économiser plusargent queeffectuer le test tandis queclients utilisent déjà.

Le Rapporttestspénétration

Une foisvous avez terminé le test, vous devez compiler toutes les données dans un format approprié et soumettre un rapport. Gardez àesprit que la majorité du personnel de gestion ne peut pas être orientéetechnique,sortele doit être divisé en sections appropriées pour faciliterlecture. Vous devriez avoir un résumé, un résumé technique contenant tout le jargonspécifique, et un résumé de gestion qui explique ce qui doit être fait pour corriger les défauts détectés.

Chapitre 3: La méthodologie du Hacker

Imaginez un soldatva dans un champbataille entièrement équipé dans les armesplus récentes etplus avancées. Ils sont pleins de confiance et savent avec certitude qu'ils vont gagner. Cependant, lorsque les combatscommence, le soldat découvre qu'ilentré dans une embuscade. Il peut descendreplupart des troupes ennemies, mais parce qu'il n'a jamais été préparé pour la bataille, il finit par perdre.

Ce scénario est pas si farfelue sion considère le nombre de soi-disant « pirates » qui ne prennent paspeinese préparer à leurs attaques. C'est là une méthodepiratage est très pratique.

Une méthodologiepiratage est ce qu'un pirate utilise pour les guider de la première étape à la dernière. Pour exploiter efficacement une vulnérabilité dans un système, vous devez identifier quelques éléments clés qui vous aiderontatteindre vos objectifs. Sans une méthodologie appropriée, vous risquez de finir par perdretemps etlutte contreénergieune bataille perdue d'avance.

Cartographie cible

Trouver la cible parfaite pour votre attaque est pas aussi simple que cela puisse paraître. Vous devez être stratégique dans la façon dont vous menez votre recherche et effectuezrecherche sur la cible avec le pluspotentiel. Vous devez analyser leurs habitudes et utiliser les informations recueillies pour trouver la stratégieplus appropriée. L'objectif de cartographier votre objectif est de déterminer quoi et qui vous attaquez avantpénétrerle système.

Pirates informatiques vont généralement après une ou plusieurs cibles àfois. Selon le type d'information que vous recherchez, vous pouvez décider d'attaquerserveurs Web stockantinformations personnelles. Vous pouvez également décider d'aller grand et pirater une institution financière. Votre cible pourrait être un site Web spécifique que vous voulez prendre àaideattaquesdéni, ou vous pouvez défigurer sa page Web. Vous pouvez être intéressé par une personneparticulier dans une organisation.

Lorsque vous êtesrecherche de cibles potentielles àattaque, vous devez considérer le niveau de sécurité que vous allez essayer de surmonter.plupartpirates vont seulement aprèscibles qu'ils connaissent sont faciles à battre,sortele niveau de vulnérabilité est souvent un facteur clé danscartographievotre cible.

Un autre facteur à considérer estsavoir si les informations obtenues de l'attaque estpeine. Cela vous aideradéterminer combientemps vous êtes prêt à prendreessayant d'accéder au système.

Alorscomment allezvous recueillirinformations sur votre cible?

- **EffectuerrechercheslIgne**

Vous pouvez Google le nom de la cible etvérifier leur compte Facebook ou LinkedIn. Cela peut faire apparaître leurs coordonnées. Si votre cible est une organisation, vous pouvez rechercher des offres d'emploi que l'entreprise a annoncés pour,particulier dans le département informatique. Vous pourriez être surpris d'apprendre à quel pointinformations utiles est donnée dans une offre d'emploi, par exemple, le logiciel querecrues potentielles doivent connaître.

Tant que hacker, vous devez savoir quels mots clés apporteront le plusinformations. Utilisezde Google *de recherche avancée* fonctionafinidentifier les sites qui ontbacklinks dans le site de votre cible. Si vous souhaitez accédertousfichiers qui peuvent être dans le site Web d'une entreprise, vous devrez utiliser un commutateur comme indiqué cidessous:

site: www.abc.com motclé

Autre technique à utiliser est l'outil WHOIS. Whois est un excellent moyen d'effectuer une attaque d'ingénierie sociale ou scannez un réseau. Vous pouvez trouver les serveurs DNS du domaine cible, ainsi que les noms et adresses des personnes qui ont enregistré le domaine cible.

Google Groupestendance à stocker beaucoup de données sensibles sur ses utilisateurs, par exemple,nomsutilisateur,noms de domaine et adresses IP.

- **Ramper Web**

Acquire ce qu'on appelle les « outilsexploration Web » pour créer une image miroir du site cible. Une foisvous avez fait cela, tousfichiers du site qui est accessiblepublic sera téléchargé sur votre disque dur local. Cela vous permettra de numériser la copie miroir ettrouvernoms etadresses email des employés,fichiers,répertoires, le code source pour ses pages web, et beaucoup plusinformations.

- **Sites**

Vous devriez maintenant être conscient qu'il ya certains sites qui sont un trésor d'informations clés surindividus etorganisations.bons exemples comprennent www.sec.gov/edgar.shtml, www.zabasearch.com et www.finance.yahoo.com.

Numérisation réseau cible

Jusqu'à présentvous avez étécollecteinformations qui vous permettra de voir l'ensembleréseau cible dans son ensemble. Les nomshôtes,ports ouverts,adresses IP etapplications en cours devraient maintenant être visibles pour vous. Rappelezque si vous êtes d'effectuer un efficace exploit, vous devez apprendre à penser comme un hacker malveillant.

Vous pouvez commencer à utiliserlogiciel de numérisation pour trouver et enregistrer toushôtes qui sont accessiblesligne. Votre propre système d'exploitation devrait avoir son propre outil de ping standard. Cependant, il existeoutils tiers comme SuperScan et outils NetScan Pro qui sont capables de ping le nomhôte du domaine ou plusieurs adresses IP simultanément.

Analyseports ouverts

Tant que débutant, il existeoutils que vous pouvez utiliser pour vérifier la présence de ports ouverts pour pénétrerle réseau cible.exemples de certains outils efficaces comprennent SuperScan, Wireshark, et OmniPeek.

Expositionvulnérabilités système

Supposant quevous trouvezcertaine vulnérabilité dans le système de votre cible, vous pouvez alors commencervérifier si ces lacunesmatière de sécurité sont exploitables. Vous pouvez suivre la voie manuelle ou utiliser un outil d'évaluation automatique.

La méthode manuelle vous demandera de créerlien versun des ports ouvertsvousdécouvert plus tôt. . Testez ces ports jusqu'à ce que vous trouviez un moyen de

la méthode automatisée implique l'utilisation d'outils tels que *QualysGuard,*qui est un outil basé sur le nuage qui est conçu pour scannerports ouverts. Un autre outil qui est disponible est Nexpose, qui peut numériser un total de 32 hôtes simultanément.

Chapitre 4: Obteniraccès physique

Imaginez: Une société de plusieurs millionsdollars investitmillions de dollars surcontremesures de sécurité cybernétique axéestechnologie pour protéger ses données. Ils ont totalement verrouillé leurs réseaux et systèmes, et ont mené plusieurs tests de pénétrationutilisantpiratesélite pourprotéger des pirates qui peuvent avoir été engagés par leurs concurrents.

Maintenantimaginez que cette société continue d'embaucher une entreprise de sécurité qui agardes de sécurité paresseux. Ils ne font jamais de contrôles physiques autourl'installation et même laisser des portes ouvertes.visiteurs sont rarement analysés ou invités àconnecter. Même les salles informatiques sont généralement laissées ouvertes.

Diriezvous que c'est une entreprise intelligente qui prend soin de protéger ses données contrepirates? Oui, ils ont branché les trous électroniques, mais ils ont littéralement laissé la porte ouverte pourpirates d'ouvrirbrèche physiquement leur sécurité!

Vous n'avez pas à pirater un réseaudistance pour accéder aux données. Vous pouvez avoiraccès physique à une installation eteffectuer votre exploit deintérieur.cours des deux dernières décennies,plupartentreprises ont constaté qu'ilextrêmement difficile de maintenirsécurité physique. Merci aux progrèsla technologie, il y a maintenantvulnérabilités plus physiques qu'un pirate peut tirer profit.

Dans le monde d'aujourd'hui des lecteurs USB, tablettes, smartphones et ordinateurs portables,plus en plusdonnées sont stockées dansappareils plus petits portables. Il est pas difficile de mettremain surtels dispositifs, en particulier compte tenu du fait queplupartemployés prennentdonnées avec eux quand ils quittenttravail à la fin de la journée. Une foisvous identifiez votre cible, vous ne pouvez pas même avoir à entrerle bâtiment; ils apporteront les données pour vous.

Dans ce chapitre, vous allezapprendre davantage surfaçon de tirer parti de certaines des failles de sécurité physique dansbâtiments que vous avez ciblés. Une foisvous avez violé la sécurité etaccès physique acquis sur place, préparezà pénétrerle système de l'intérieur.

Types de vulnérabilités physiques

- non d'établir une réception pour surveillervisiteurs qui entrent et sortent du bâtiment.
- non-application signature dans obligatoire de tousemployés etvisiteurs.
- employés etpersonnel de Distant sécurité qui ne sont pas complètement familiers avec les réparateurs informatiques,fournisseurs oufournisseurs.
- Jetant documentsentreprise et personnels sensibles à la poubellelieu de les déchiqueter.
- non-verrouillageportes menant àsalles informatiques.
- Laissantappareils numériquestrouvant dans les bureaux.
- défaut de fixerportes qui ne peuvent pas fermer correctement.

Créer votre plan

une des premières chosesvous aurez à faire est de trouver un moyen d'atteintesécurité physique. Cela nécessitera un travail vaste de reconnaissance de votre part. Vous devez identifier le type de mesures de sécurité que l'installation a mis en place, les faiblesses etvulnérabilités présentes, et commenttirer profit.

Cela peut sembler simple surpapiermais il est pas si facile une foisvous obtenez sur le terrain. L'hypothèse ici est que vous travaillez sans hommeintérieur de vous nourrir les informations vitales de sécurité. Ilpeutêtre deuxtrois semaines avantvous êtesmesure de recueillir toutes les informationsvous avez besoin pour lancer votre attaque. Une atteintela sécurité physique signifievous devez avoir les compétences etconnaissances nécessaires pour non seulement entrerle bâtiment, mais aussi pour manœuvrer votre cheminintérieur, puissortie sans être détecté.

Si vous manque la patience,condition physique etagilité mentale nécessaire pour une telle tâche, alors ne pas tenter une violation physique. Tenezd'effectuer vos attaques à distance.

Il y a un certain nombre de facteurs de sécurité physiquevous devrez tenir compte lorsplanification comment accéder à votre cible. Ceuxci sont classés en deux catégories distinctes:contrôles physiques etcontrôles techniques.

Contrôles physiques

Vous aurez à prendrecomptefaçon dont les contrôles deéquipe de sécurité, surveille et gèreaccès dans et hors de l'établissement. Dans certains cas, le bâtiment peut être divisé en sections publiques, privées et restreintes. Vous devrez déterminer la meilleure technique pour entrerla section qui contient la cible.

1. Périmètresécurité

Comment prévoyez-vous contourner la sécurité du périmètre? Vous aurez besoin de savoir si l'installation comporte un mur,clôture,chiens,caméras de surveillance, tourniquets, etautres sas types de périmètresécurité. Cesont que les moyensdissuasion que vous pourriez avoir à traiter à l'extérieur. Une installation bien gardé auracouches de sécurité secondaires que vous obtenez plus près du bâtiment.

À ce stade, vous devez savoir où sont les faiblesses dans la conception

de l'installation. S'il y a un haut mur qui agrands arbres tout autour, vous pouvez monter les branches et sauter dans le composé. Bien sûr, vous devez être physiquement agile et assezforme pourfaire.

Apprenez l'emplacement des feux de sécurité et où les taches sombres ouombres tombent. Ceuxci peuvent fournirgrandes cachettes si vous prévoyez d'avoir accès la nuit. Vous devriez également considérer dumpster diving comme un moyen d'accéder àdonnées sensibles. Vérifiez l'emplacement des bennesordures et si elles sont facilement accessibles. Ce serait une bonne idée de savoir quand les ordures sont collectées afin que vous puissiez faux faire partie de l'équipage des ordures.

1. Badgesidentification

Organisations utilisentbadges d'identification etID utilisateur pour surveiller et contrôler le mouvement des employés. Ils sont également utilisés pour suivre les fichiers etrépertoires qu'un employé crée ou modifie. Mettremain sur un badge d'identification peut vous obliger à voler un d'un employé légitime, oufaire votre propre insigne faux. Si vous ne pouvez pas obtenir un badge d'identification, alors vos autres options seraient:

- Entreztant que visiteur et votre escorte échapper.
- Utilisez la technique talonnage,supposant que le bâtiment ne dispose pasun mantrap.
- Befriend un employé dans la zone fumeurs et les suivreque vous continuez votre conversation.
- Obtenez un uniforme faux et usurperidentitéun entrepreneur,vendeur ou réparateur. Si vous voulez aller all-in, puis envisageracquisitionun camion de service etéquipement pour vous faire paraître plus légitime.

1. systèmesdétectionintrusion

Ces facteurs comprennent généralementdétecteurs de mouvement etalarmes d'intrusion.

Vous devrez connaître les types de détecteurs de mouvementvous traitez. Sontilsinfrarouge,base de chaleur, forme d'onde, capacité, photoélectrique ou détecteurs de mouvement audio passif? Chacune de ces œuvres différemment et comprendre ses forces et ses faiblesses vous aidera dans votre mission.

Vous aurez également besoin de connaître le type d'alarmeintérieur du

bâtiment. L'installation peut avoircapteurs sur les portes etfenêtres, détecteurs de bris de verre,capteurs d'eau, et ainsisuite. Alors que certaines alarmes sont destinées à informer silencieusementsécurité d'une violation potentielle,autres sont conçus pour dissuader ou repousser l'attaquant. Une alarme de dissuasion fermeraportes et activer serrures pour sceller tout et toutmonde. Une alarme répulsive ferabruits forts et émettentlumières vives pour essayer de forcer un attaquant hors du bâtiment.

Contrôles techniques

Ce sont généralement concentrés surcontrôleaccèscar il est la zoneplus vulnérable desécurité physique.contrôles techniques comprennentcartespuce etcamérasvidéosurveillance.

1. cartespuce

Ces puces électroniques ontcircuits intégrés et qui traitentdonnées et permettent une authentificationdeux facteurs.cartespuce contiennentinformations des employés et les domaines de l'installationils sont autorisés / non autorisés à accéder. Avoir la carte seule ne vous aurez accès à une installation. Un scanner biométrique et NIP / motpasse doivent également être utilisés pourauthentification. Cependant,cartespuce ont certaines vulnérabilités.

Une méthodede contournercartespuce est par *génération de*défaut.C'est làvousingénierie inverse du cryptage afin de trouver la clé de cryptage etaccéder aux données stockées. Cela impliquesaisieerreurscalcul en modifiant la fréquence d'horloge ettension d'entrée oumodifier les variations de température.

Vous pouvez également utiliser une attaque à canal latéral pour comprendre le fonctionnement decarte sansendommager. Cela impliqueexpositionla carte à des conditions différentestraversanalyse électromagnétique,analyse de puissance différentielle, etsynchronisation.

Autre façon est d'utiliserlogiciel pour effectuer une attaque non invasive. Cela impliquepiratage des commandes logicielles etchargement qui vous permettent d'extrairedonnées de compte. Enfin, il existe un procédé connu sousnom *micro-sondage.*Ceci est une attaque intrusive qui consistereliersondes directement sur la puce. L'objectif est de prendre la puce et remettrezéro ici.

1. Camérasvidéosurveillance

La norme de surveillance vidéo estcamérasvidéosurveillance. Ils sont situés àendroits stratégiques et sont surveillés paragents de sécurité assis dans une salle de contrôle. Cependant, il y a toujourstaches aveugles à exploiter, vous devez donc savoir où ceuxci sont. Les caméras peuvent être sans fil ou surWeb,qui signifievous pouvez pirater l'alimentation decaméra etmanipuler les images sont affichées surécran ou brouiller le signal.

Sécurité physique est un élément essentiel desécurité cybernétique.pirates informatiques chercheront toujours à toute faiblesse qu'ils peuvent trouver, quesoitligne ou hors ligne.

Chapitre 5:ingénierie sociale

Saviezvous que l'année 2016, les trois principales préoccupations cyber-menaces étaientingénierie sociale,menaces internes etmenaces persistantes avancées? Cela vous montre à quel pointattaques d'ingénierie socialesévissent sont devenus en cybersécurité.

Pourquoi pensez-vous ingénierie sociale est numéro un sur cette liste? Un pirate est censé attaquer le système ouréseau, alors pourquoi ilsconcentrer sur un autre aspect du système de sécurité d'une organisation?

La réponse réside dans le peuple. La plus grande faiblesse de touséléments de sécurité sont les personnes impliquées. Nous avons vu dans le dernier chapitre comment la technologieplus avancée ne peut vous protéger contre les cyberattaques si les personnesgardaient le bâtiment dorment au travail. Grâceingénierie sociale, vous pouvez pirater les gens en gagnant leur confiance etles exploiter pour les informationsvous avez besoin. Cependant, vous aurez besoinun certain degré d'audace ethabileté pour amenergens à vousconfiance, étant donné que vous êtes un étranger.

Unaspects deingénierie sociale est qu'il est généralement fait avec un hack de sécurité physique. L'objectif est de prendre contact avecpersonne qui ainformations spécifiques qui peuvent vous aideraccéder aux fichiers ouressources de votre cible.

Par exemple:

- Envoyer la cible un email contenantliens. Quand ils cliquent sur le lien,logiciels malveillants ouun virus est téléchargé sur leur ordinateur, vous permettant ainsi de contrôler le système etacquisitiondonnées.

- Si vous êtes un employé dans une entreprise etvous voulez obteniraccès non autorisé àdonnées confidentielles, vous pouvez informer le service de sécurité que vous avez perdu votre badge d'accès. Ils vous donneront les clés pour entrerla salle vous permettant ainsi d'obtenir les fichiers physiques et numériquesvous voulez.

- Vous pouvez usurperidentitéun fournisseur de produit authentique et prétendre que votre entreprisebesoin de mettre à jour ou installer un correctif sur le logiciel du client (par exemplelogiciel de comptabilité). Vous pouvez alors demander à donner le mot de passe administrateur. Sinon, vous pouvez

simplement leur demander de télécharger le logiciel faux, qui vous donnera accèsdistance au réseau de la cible.

Ces exemples peuvent sembler trop simple ou facile, mais rappelezvous queingénierie sociale est la tactiqueplus utilisée parpirates pour violersécurité cybernétique. En apprenant commentpirates malveillants commettent leurs exploits, vous êtes mieux placé pour empêcher votre propre système, ouautres, d'être piraté.

Stratégiesingénierie sociale

Examinons en détail quelquesunes des stratégies quepirates utilisent lors d'une attaque d'ingénierie sociale.

1. Gagnerconfiance

Une des meilleures façons de construireconfiance pour un outil d'ingénierie sociale esttraversmots etactions. Vous devez être articulé, forte, et être un bon causeur. Il y acas où un ingénieur social échoue dans sa mission parce qu'ils ont été négligents dans leur discours ou ont agi nerveusement. Cela arrive souvent quand le pirate affiche les signes suivants:

- Parler trop ou montrer tropenthousiasme
- intérim nerveusement en réponse àquestions
- Poserquestions bizarres
- comparaissent à être pressé
- informations Ayant seulement réservé aux initiés
- Parler des gens dans la haute directionseinl'organisation
- Pretending comme ils ontpouvoirseinla société

Tant que vous pratiquezbonnes compétences en ingénierie sociale et techniques, vous serez en mesure de cacher ces signes.

Une tactique très efficace à utiliser pour gagner la confiance de quelqu'un est de sortir de votre façon de faire une faveurquelqu'un et demander immédiatement un en retour.autre tactique est quelque chose que vous avez probablement vu dans un film. Vous définissez quelqu'un en créant un problème particulier pour eux. Lorsque la victime crie àaide, vous précipitez sur la scène etles enregistrer. Cela fonctionne pour créer un lien entre vous et la cible potentielle.

Un travail fausse carteidentité et uniforme peuvent parfois vous aiderusurperidentitéun employé dans une entreprise, vous permettant ainsi d'entrerl'établissement non détecté.gens vont même vous donnermotspasse et autres informations sensibles aussi longtemps que vous semblez êtreun d'entre eux.

1. Phishing

Piratesqui utilisentattaques d'ingénierie sociale sontmesure d'exploiter leurs ciblesutilisanttechnologie car il est plus facile et plus amusant.gens peuvent être très naïf surtout quand ils sontligne. Il est tout simplement incroyablecomment faire confiancegens sont en ce

jour etâge de plusplus des cyberattaques.

Phishing consisteenvoyeremails cibles qui semblent provenirune source légitime ouconfiance. L'objectif est de les amener à partagerinformations sensibles ou personnellessoit enenvoyant directement oucliquant surliens.

L'email ressemblerala vraie affaire de la cible viséemais c'est parce que vous avez falsifié l'adresse IP pour afficher une adresse email qui semble authentique. Vous pouvez faire semblant d'être un ami,parent oucollègue etleur demander de vous envoyer leurs renseignements personnels.

Vous pouvez également faire semblant d'être une institution financière et demandezleur de cliquer sur le lien afin de mettre à jour leurs informations de compte. Quand ilsfont, ils seront dirigés vers un faux site Web qui reflète le vrai. Comme ilsconnectent, vous pouvez accéder à leurs nomsutilisateur, ID utilisateur, motspasse, numéro de compte bancaire, ounuméro de sécurité sociale.

Spamming estautre tactiquevous pouvez effectuer. Vous venezles envoyer une tonne de courriels etattendre qu'ils deviennent curieux et ouverts au moins un d'entre eux. Le courriel contiendra une demande de téléchargement en échange de certaines informations personnelles un cadeau gratuit (ebook, vidéo, coupon, etc.).

Une des figuresplus courantes consiste à prétendre être un fournisseur de logiciel vérifié. Toutvous avez à faire estenvoyer la cibleun correctif logiciel par email et leur demander detélécharger gratuitement. Ce qu'ils ne réalisent pas est que le logiciel estfait un chevalTroie ouporte dérobée qui vous permet d'avoircontrôle complet de leur système.

Escroqueriesphishing fonctionnent si bien parce qu'ils sont très difficiles à retracer au pirate. Les outils queingénieurs sociaux utilisent, par exemple, réexpéditeurs etserveurs proxy, fournissentanonymat suffisant pour les empêcher d'être découvert.

Comment prévenir une ingénierie sociale Hack

Comme un pirateherbe, vous êtes probablement plus intéressés à apprendre comment effectuer une attaque plutôt queprévenir. Cependant, comme nousdisions au début,piratage peut travaillerfois pourbien et pourmal. Il est donc important que vous comprenez comment une attaque peut être évitée afin que vous pouvez conseillerun clientconséquence. Ces informations seront également vous aiderréaliserexploits plus efficaces. Après tout, il n'y a pas besoin de perdretemps eténergieattaquer la cibleutilisant une technique qu'ils ont déjà protégé contre.

Organisations utilisent généralement deux techniques pour empêcheringénieurs sociaux d'exploiter leurs vulnérabilités:

1. **développement etapplicationpolitiques strictes** - L'organisation peut créerhiérarchies deinformation, oùutilisateurs sont autorisés à accédercertainesmais pas toutesdonnées. Il devrait égalementavoirapplication stricte de porterbadges d'identification par tousemployés et consultants, et chaque invité doit être escorté parsécurité. Lorsqueemployés licenciés,traitants ou fournisseurs quittent les lieux, ils doivent être dépouillés de leurs papiersidentité. Le même motpasse doit pas être utilisé pendant plus d'une durée déterminée. Enfin, dans le cas où un comportement ou manquement suspect est détecté, il doit y avoir une réponse rapide par le personnel de sécurité. L'aspectplus important de toute politiqueorganisation estrespect. Les personnes concernées doivent comprendre les exigences et les suivre en tout temps.
2. **Formation des utilisateurs en sensibilisationla sécurité** - plupartemployés ne savent pas quoi faire quand ils sont confrontés à une attaque d'ingénierie sociale. Il doit y avoir une sorte de sensibilisation des utilisateurs etformation afin d'enseignergens comment identifier et répondre aux pirates. Cette formation doit être continue plutôt qu'un événement ponctuel. Le programme de formation devrait être assez facile pour ceux qui ne sont pas techniquement d'esprit pour comprendre. Il est également important pourgestionnaires supérieurs à donner l'exemple et s'engagent aussi la formation.

Depuisattaques d'ingénierie sociale ne sont pas seulement destinés aux organisations, nous devons examiner commentindividus peuvent se protéger. Certains des moyens de prévenir ce genre d'attaque comprennent:

1. Évitezdonner des motspasse àgenshasard.
2. Évitezenvoyer vos informations personnelles par email oumédias sociaux sans vérifier l'identité du récepteur. Assurezvous que vous savez qui vous envoie une demande d'ami ouconnexion sur Facebook, LinkedIn, ou Twitter.
3. Évitez téléchargerpièces jointespartiradresses IP non identifiées, oucliquant surliens danscourrier spam.
4. Évitez la tendance à passer votre curseur sur un lien email.pirates informatiques sontmesure d'intégrerlogiciels malveillants dans un lien et déclencher un téléchargement moment la souris passe dessus. Anti-Malware est un bon moyen d'éviter ce type de hack.

La vérité est que siingénierie sociale peut être un peu compliqué à enlever,empêche il est également très difficile. Une organisation ne peut pas contrôler toutes les personnesliées en tout temps, ettant qu'individus, chacun a sa propre faiblesse unique. Il est votre travail pour trouver et exploiter.

Chapitre 6: Piratagemotspasse

Une des façons les plus communes pour assurer la sécurité de vos données estmot de passe-protéger. Nous sommes devenus tellement habitués à mettremotspasse dans tous nos appareils numériques que nous croyonsfait que cette mesure est suffisante pour garder nos informationstoute sécurité.

Cependant, la vérité est très différente.motspasse font un bon travail de garderutilisateurs non autorisés d'un systèmemais comme noussavons tous,pirates malveillants ont étémotspasse ayant une fissuration journée surterrain. Dansplupartcas, un utilisateur peut même pasrendre compte que quelqu'unautre estcourant de leur motpasse.motspasse peuvent rendregenssententsécurité, mais il y a un certain nombre de vulnérabilitésseinleur qu'un pirate peut facilement exploiter.

Types de vulnérabilités de mot de passe

Il y a généralement deux types de vulnérabilités de mot de passe: *User* et technique.

Vulnérabilités deutilisateur

Vulnérabilités deutilisateur sont les faiblesses qui résultent deabsence de politiques de motpasse approprié ou la faible application de ces lignes directrices. Par exemple, combien de fois vous avez vu quelqu'un utiliser le même motpasse pour leur ordinateur portable, smartphone, tablette, et tous leurs appareils numériques? Imaginez quelqu'unutilisant le même motpasse pour leur Yahoo, Gmail, LinkedIn, Facebook, et Twitter! Il n'y a pas besoin d'imaginer parce que c'est exactement ce queplupartgens!

La majorité des gens trouvent simplement trop difficile à mémoriser chaque motpasse unique. Nous vivons dans un monde de complaisance,sorteplupartgens juste pour regarder les plus rapides et plus faciles à faire avancerchoses. Celatraduit généralement pargens répéter le même motpasse pour tous leurs comptes. Malheureusement, cela a simplement fait le travail des pirates beaucoup plus facile.

Avec toutes les lettres etchiffres disponibles pourutilisation, il existe potentiellement trois billionscombinaisons de mot de passe, huit caractères. Pourtantvous seriez surpris dele nombre de personnes qui choisissentmotspasse faibles et stupides juste pourrendre plus facile bachotage. Certainsmême nesoucient pasmotspasse et sauter le processus toutfait!

Alorsquelles sont quelquesunes des vulnérabilités des utilisateurs qu'un pirate peut tirer profit?

- motspasse qui ne sont jamais modifiés.quand remonte la dernière foisvous avez changé votre motpasse Twitter oucourriel? Pourquoi passer par les tracas, non?
- Le même motpasse utilisé dans plusieurs comptes différentstravers différents réseaux et systèmes.
- motspasse trop simples et sont liés à votre nom,emplacement,école,emploi, et ainsisuite.plupartutilisateurs regardent juste la salle lorsqu'on luidemandé de créer un motpasse. Peu importe ce qu'ils voient est ce qu'ils vont utiliser. Cela peut paraître drôlemais il est vrai.
- motspasse qui sont longues et complexes sont généralement écrits surmorceaux de papier ou stockés dans un fichier. Tant

que l'emplacement du fichier est non sécurisé, il peut être volées.

Vulnérabilités techniques

Exploitantvulnérabilités des utilisateurs est généralement la première étape pour un pirate informatique. Après cela, vous essayez de voir s'il y a des faiblesses techniquesvous pouvez tirer profit. Les plus courantes sont:

- non-utilisationapplications qui masquent le motpasse car il est tapé sur l'écran. Bien queplupartapplications cachent immédiatement les caractères dactylographiés sur l'écran, certains nefont pas. Si un utilisateur n'a pas configuré les paramètresmanière appropriée, ils se laissent vulnérables aux *surfeurs d'épaule* (ceest expliqué plus loin).

- utilisantprogrammes oubasesdonnées pour stocker tous vos motspasse, maisdéfaut d'obtenir la basedonnées appropriée. Certains utilisateurs stockent tous leurs motspasse dans un MS Word, Access ou fichier Excelmais ne parviennent pas à sécuriser le document luimême.

- utilisation de basesdonnées non chiffrées accessibles pargrand nombre de personnes non autorisées. Cela est souvent le cas avecorganisations.

- utilisation de techniques de cryptage faibles paréditeurs de logiciels etdéveloppeurs. La plupart des développeurs ont tendance à avoirtrop grande confiance dans le fait que leurs codes source sont inconnus. Ce qu'ils ne réalisent pas est queavec asseztemps etpatience, tout pirate expérimenté peutfissurer un code source. Un pirate qui a assezpuissance de calcul peut même utiliseroutils conçus pour pirater chiffrements faibles.

Comprendre Motpasse cryptage

Un motpasse est dit être crypté lorsqu'il est stocké dans un système utilisant un cryptage ou un moyen algorithme de hachage. Une fois le motpasse est haché, un utilisateur voit tout est une chaîne cryptée de longueur fixe. L'hypothèsebase est qu'une fois un motpasse a été haché, il ne peut pas être fissuré. LINUX va encore plus loin et ajoute une valeur aléatoire (un sel) au mot de passe haché, juste pourrendre plus sûr. Le sel est ce qui permet à deux personnes d'utiliser le même motpasse exactement encore génèrentvaleurs de hachage totalement différentes.

Il y a un certain nombre d'outils qui peuvent être utilisés parpirates pour cassermotspasse. Ces outils fonctionnent en prenant plusieurs motspasse bien connus,les exécuter par un algorithme de hachage, puis générer hash crypté. Une foisles hash chiffrés ont été générés, l'outil les compare au mot de passe qui doit être craqué. Bien sûr, ce processus se produit à une vitesse très rapide, et le motpasse est fissuré le moment le hachage original et la correspondance de hachage cryptée.

Parfoisun pirate peut trouver un motpasse qui est très complexe et forte. Ces motspasse sont assez difficiles à craquer, mais avec les bons outils, le temps etpatience suffisante, tousmotspasse peuvent être piraté. Si vous voulez vous assurer que votre système estabri des pirates, vous devez obtenir les mêmes outils qu'ils utilisent, rechercher votre système pourvulnérabilités et les corriger.

Outils-Cracking Motpasse

Il y a beaucoup d'outils avancés sur le marchéce moment pourcraquagemotspasse. Certains sont plus populaires queautresraison de leur efficacitétravers divers systèmes et logiciels d'exploitation. Par exemple:

- **Ophcrack** - Cet outil est utilisé pourcraquagemotspasse dansapplications Windows.
- **Caïn et Abel** - C'estun des outils les plus efficaces. Il peut être utilisé pourcraquage hash,motspasse VNC et Windows, et bienautres applications.
- **John the Ripper** - C'estaucun douteun des plus connus et aimés programmes pourcraquagemotspasse. Il combine un style dictionnaire d'attaque avantlancer une attaque de force brute totale. Il est utilisé pourcraquage LINUX et motspasse Windows haché.
- **Brutus** - Cet outil fonctionne bien pourcraquageconnexions pour HTTP, FTP, etc
- **Elcomsoft Distributed Password Recovery** - Cet outil fonctionne extrêmement rapide en intégrant un programme d'accélération vidéo GPU etutilisantmilliers d'ordinateursréseaumême temps. Il est capable defissurerWindows, Adobe, iTunes etautres applications.
- **Elcomsoft System Recovery** - Cet outil utilise un CDdémarrage pour réinitialiser les droitsadministrateur sur un système Windows.

Il y a beaucoupautres outils que vous pouvez utiliser pour piratermotspasse sur une variété d'applications,systèmes etréseaux. La choseplus importante est de comprendre comment fonctionnechiffrement et comment ces outils peuvent être utilisés pour surmonter le chiffrement.

Techniques de craquagemotspasse

Nous avons tous essayé à un moment donné pour casser un motpasse. Cela aurait pu être l'ordinateurla maison, dans le laboratoire deécole, ou peutêtre l'appareil d'un ami. Il est probable que vous avez utilisé une méthode classique plutôt qu'une avancée. Les techniques cidessous sont une combinaison de certaines approchesvieille école et des méthodeshaute technologie.

1. **Deviner** - Ceci est probablementune des techniquesplus galvaudé. Il est également l'approchesimple puisqueplupartutilisateurs ont tendance à choisirmotspasse dont ils se souviendront facilement. Toutvous devez faire est logique d'utiliser pour deviner ce qui peut avoir été utilisé pour créer leur motpasse. Cette technique fonctionne mieux lorsque vous connaissez la cible ou ontaccès facile à leurs données personnelles. Le motpasse est souvent le nom de l'utilisateur ou un membre defamille, leur carteidentité, leur anniversaire, ou même leur animal préféré.
2. **Piquage** - C'est là vousmain autourune personne qu'ils clé dans leur motpasse. Vous pouvez regarder les caractères à l'écran oumémoriser leurs frappes. Il est important que vous mélanger pour éviterdétection, et être discret sur vos mouvements. Si vous souhaitez obtenirmotspasse des personnes dans un lieu public comme un café, vous pouvez placer une caméra dans un endroit stratégique pour surveiller leurs frappes de connexion.
3. **Ingénierie sociale** - Que faire si vous pourriez obtenir un motpasse en demandant simplement pour cela? La grande majorité des gens ont tendance à croire ce qu'on leur ditparticulier si elle est dans un cadre officiel. Vous pouvez littéralement avoir accès aux dossiers des employés de partout ces jours, grâce aux médias sociaux etsites Web deentreprise. Un pirate peut usurperidentitéun membre du personnel du service informatique d'une entreprise, appeler un utilisateur, etles informer de quelques accrocs techniquessein du système de messagerie. Le pirate demande alors que l'utilisateur leur donne leur motpasse pour régler le petit problème.
4. **Attaquesdictionnaire** - C'est là un programme est utilisé pour créer une liste de mots de dictionnaire de texte qui

peut être comparé au motpasse réel. Il implique hachantmots en texte brut, salage, puis les comparer au mot de passe de l'utilisateur. Le mot qui correspond est alors considéré comme le mot de passe de l'utilisateur.programmes qui peuvent vous aiderlancer une attaquedictionnaire comprennent *John the Ripper, LophtCrack* et *Caïn et*Abel.

5. **Attaques de force** - Cela ne devrait jamais être votre premier choix en matière de craquageun motpasse. Il est une technique inefficace et extrêmement chronophage. Il est considéré comme une option de repli qui est utilisé lorsque toutesautres méthodes ont échoué. Il est principalement utilisé pour cassermotspasse6 caractères ou moins,qui estraisonlaquelle vous êtes toujours conseillé de faire vos motspasse8 caractères ou plus. Pluscaractères qu'un utilisateur met dans son motpasse, plus il est difficilese fissurerutilisant une attaque par force brute. Cependant, une attaque de force brute est très exhaustive,qui signifie que tôt ou tard le motpasse sera fissuré. Malheureusement, personne ne peut prédire quand cela se produira.programmes qui utilisent cette technique comprennent *John the Ripper, Rarcrack* et Oracle.

Les méthodes cidessus sont les moyenssimples etplus couramment utilisés pour cassermotspasse. Il existeautres approches qui sont disponibles, par exemple,matrice etmotpasse de probabilité tables arc en ciel. Cependant, pour un débutant, ce serait tout simplement trop complexes pourici.

Utilisant John the Ripper et pwddump3 pour casser un motpasse

L'outil pwdump3 est un moyen efficace pour extrairemotspassepartirune basedonnées hachés Security Accounts Manager. John the Ripper, comme indiqué précédemment, peut travailler surdeux motspasse Linux et Windows. Cette procédure exige que vous avezaccès administratif.

Si vous essayez de casser un système Windows, procédezsuit:

1. Sur l'ordinateur, allez surlecteur C. Créer un répertoire et appeler«motspasse. »
2. Assurezvous que vous disposezun outil de décompression (tel que WinZip) installé sur l'ordinateur.cas contraire, puis téléchargez et installez.

3. Télécharger pwdump3 et John the Ripper et les installer immédiatement. Les extraire dans le répertoire créé cidessus.
4. Tapez la commande

c: passwordspwdump3 > cracked.txt

La sortie de cette étape seramotpassecomptessécurité Windows Gestionnaire hash, qui sera ensuite capturé dans le fichier txt.

1. Tapez la commande

c: craked.txt passwordsjohn

Ceci lancera John the Ripper contre les hashs, et la sortie seront les mots de passe utilisateur fissurés. Cependant, ce processus peut prendre un temps très long, selon la complexité des motspasse sont et le nombre d'utilisateurs du système.

Si vous Cracking un système LINUX, utilisez la procédure suivante:

1. Télécharger les fichiers source pour LINUX.
2. Tapez la commande

[root @ yourcurrentfilename hôte local] #tar - zxf john - 1.7.9.tar.gz

Cela va extraire le programme et créer un répertoire / src.

1. Dans le répertoire / src, tapez la commande

make générique

1. dans le répertoire / Exécuter, tapez la

commande./ unshadow / etc / passwd / etc / shadow > cracked.txt

Le programme unshadow sera utilisé pour fusionnerfichiers masqués etmotspasse et lesdans le fichier txt.

1. Tapez la

commande:./ John cracked.txt

Cela va lancer le processuscraquage, qui peut également prendre un certain temps. La sortie devrait être la même que pour la procédureWindows.

Créationmotspasse sécurisés

En ce qui concernerenforcementla sécurité des donnéesseinune organisation, il devient nécessaire d'embaucher un chapeau blanc pour aiderconcevoirmeilleures politiques de mot de passe. L'objectif est d'enseigner aux utilisateurs du système comment créermotspasse plus sûrs, ainsi que les effets d'mauvaise sécurité des mots de passe. Pourpersonnes qui veulent obtenir leurs renseignements personnels, les mêmes techniques peuvent également appliquer dansplupartcas.

Les critères à suivre comprennent:

- motspasseformage qui combinentlettres majuscules et minuscules,chiffres,symboles etcaractères spéciaux.
- Ajoutsignes de ponctuation entre mots séparés
- Délibérément motsfauteorthographe
- Changermots toussix à 12 mois. En cas de violation desécurité, les motspasse doivent être changés.
- Veillerce quemotspasse sont de longueurs différentes pour rendre plus difficilefissuration.
- stockagemotspasse tous dans un programme de gestion de mot de passe plutôt queun non garanti MS Excel, Access ou fichier Word.
- Éviter la tendance à recycleranciens motspasse.
- Veillerce quemotspasse ne sont pas partagés du tout, pas même avecamis ou des collèguestravail.
- Verrouillage du BIOS systèmeaideun motpasse
- Etablirméthodes d'authentification plus avancées, par exemple,certificats numériques oucartespuce.

Pour pirater un motpasse, vous devez comprendre ce qu'est un motpasse fort ou faible ressemble. Avoir la bonne connaissance defaçon de créer un motpasse vous aideradevenir un hacker plus efficace.

Chapitre 7: Réseau sans fil Attacks

Réseaux sans fil sont devenus tellement banalnos jours, mais malheureusement, ils sont aussi très vulnérables aux menacespiratage. Cela est dû au fait qu'ils impliquent la transmission de données par fréquences radio, rendant ainsiinformations susceptiblesêtre interceptées. Danscas où l'algorithme de chiffrement est faible oudonnées transmises sont non chiffrées, la situation devient bien pire.

Attaques WLAN

Il y a plusieurs façons qu'une attaque réseau sans fil peut être lancé. Ceuxci comprennent:

1. **Association Unintentional**

Il y acas où un réseau sans fil chevauche un autre,permetun utilisateur de sauterinadvertance d'un dans l'autre. Si un pirate malveillant profite de cela, ils pourraient acquéririnformation contenue dans un réseau qu'ils ne visent à être sur en premier lieu.

1. **Réseaux non conventionnels**

Ce sontréseaux qui ne sont pas la sécurité appropriée qui est habituellement réservé pourordinateurs portables etpoints d'accès. Ils ont tendance à êtrecibles faciles pourpirates. Ils comprennentimprimantes sans fil, lecteurs de codesbarres, périphériques Bluetooth etPDA.

1. **Des attaquesdéni de service**

Ce type d'attaque consisteenvoyercentaines oumilliers de messages, commandes ou demande à un point d'accès. En fin, le réseau est forcé de tomberpanne ouutilisateurs sont empêchés d'accéder au réseau.

1. **Man-in-the-middle**

Cette attaque implique un hacker utilisant leur ordinateur portable pour agir comme un point d'accès doux et attirerutilisateurs. Le pirateconnecte leur point d'accès doux au point d'accès réeltravers une carte sans fil différent.utilisateurs qui tentent d'atteindre le véritable point d'accès sont donc obligés de passer par le point d'accès doux. Cela permet au pirate de saisir toutesinformations sont transmises dans le réseau. Attaques Man-in-the-middle sont habituellement effectuées dansparties communes qui onthotspots sans fil.

1. **Usurpationidentité MAC**

Cela peut être décrit commevol de l'identité d'un ordinateur qui possèdeprivilèges du réseau. Un pirate tente de voler l'adresse MAC

(Media Access Control) d'un ordinateur autorisé parlogicielcoursexécution que « renifle » it out. Une foisle pirate trouve ces ordinateurs administratifs et leurs papiersidentité, ils utilisentautres logiciels qui leur permet d'utiliser ces adresses MAC.

Vérification des réseaux sans fil

La majorité des réseaux sans fil sont sécurisés parmotspasse afin de contrôlerfaçon dontutilisateurs accèdent et utilisent le réseau. Deux façons d'authentificationun réseau sans fil *Wired Equivalent Privacy (WEP)* et *Wi-Fi Protected Access (WAP)*.

Wired Equivalent Privacy (WEP)

WEP offre la plus grande intimitéun réseau câblé et crypte toutesdonnées transmises sur un réseau. Cependant,raison de ses nombreuses vulnérabilités, il a été largement remplacée par WPA.

Cracking un réseau WEP peut se faire soitactive ou passive. Fissuration active est plus efficace, provoque une surcharge du réseau, et est donc plus facile à détecter. Fissuration passive, d'autre part, ne modifie paschargetrafic jusqu'à ce que le réseau a été fissuré.

Les outils que vous pouvez utiliser pour casser un réseau WEP incluent:

- **wepcrack** - Ceci est un outil open-source que vous pouvez téléchargerpartir wepcrack.sourceforge.net.
- **Aircrack** - Cet outil vous permet de renifler un réseau, et peut être téléchargépartir aircrack-ng.org
- **WebDecrypt** - Cet outil utilise une attaquedictionnaire pour générerclés WEP. Il peut être téléchargépartir wepdecrypt.sourceforge.net
- **Kismet** - Ceci est un outil qui peut être utilisé à plusieurs fins différentes, comme reniflerpaquets réseau, détecterréseaux visibles et invisibles, et aussiidentifierintrus.

Wi-Fi Protected Access (WAP)

Cette authentification a été conçu pour surmonter les faiblesses du WEP. Cela dépend de passphraseschiffrement des paquetsutilisanttouches temporelles. Une faiblesse du WAP est qu'il est vulnérable aux attaques de dictionnaire si faibles sont utilisésphrases secrètes. Les outils de craquage WPA comprennent:

- **Cain et Abel** - Cet outil décodefichiers reniflé parautres programmes
- **CowPatty** - Cet outil utilisetactiques de force brute pour casserclés pré-partagées

CommentMAC spoofing Attacks

Un des moyens les plus populaires de prévenir une MAC attaque par usurpation consiste à utiliserfiltrage MAC. Un filtre MAC est utilisé pour bloqueradresses MAC non autorisées dejoindreun réseau sans fil, même si l'utilisateur a le motpasse. Cependant, il est un moyen efficace de bloquer un pirate déterminé.

Dans l'exemple cidessous, vous apprendrez à usurper l'adresse MAC d'un utilisateur qui a l'autorisationse connecter à un réseau. Assurezvous que votre adaptateur Wi-Fi est en mode de surveillance. Les outils qui seront utilisés sont *Airodump-ng* et macchanger.

1. Avecadaptateur en mode de surveillance, tapez la commande

Airodump-ng-c [channel] [routeur cible MAC Addres] -bssid -I wlan0mon

Cela vous permettra de détecter la cible réseau sans fil. Tousutilisateurs qui utilisent le réseau seront affichés dans une fenêtre popup, y compris leurs adresses MAC autorisées.

1. Choisissezune des adresses MAC à utiliser comme votre propre adresse. Cependant, vous devezabord éteindreinterface de surveillance. Tapez la commande

Airmon-ng arrêter walnomon

1. Vous devez alors éteindre l'interface sans fil de l'adresse MACvous avez choisi. Tapez la commande

ifconfig wlanO versbas

1. Maintenantil est temps d'exécuter le logiciel Mcchanger. Tapez la commande

macchanger -m [Nouvelle adresse MAC] wlan0

1. Allumez l'interface sans fil de l'adresse MACvous aviez choisi. Tapez la commande

ifconfig wlanO up

Vous avez changésuccès votre adresse MAC à celle d'un utilisateur autorisé.connecter au réseau sans fil et voir si vous êtesmesure deconnecter.

Comment sécuriser un réseau sans fil

Il y a un certain nombre d'approches que vous pouvez utiliser pour sécuriser un réseau sans fil. Chaque hacker éthique doit connaître ces conseils afin qu'ils puissent empêcherpirates malveillants d'exploitervulnérabilités du système. Ceuxci comprennent:

- Installerparefeu, anti-virus et anti-spyware. Assurezvous que tous vos logiciels de sécurité est misjour et le parefeu est activé.
- Chiffrez vos stations de base,routeurs et points d'accès en brouillant vos communications réseau. Ces appareils sont fabriqués aveccommutateurs de chiffrement, mais ils sontmais sont généralement éteints. Assurezque vous activez la fonction de chiffrement.
- Modifier le motpasse par défaut du routeur sans fil. Veillerce qu'ils sont longues et complexes.
- Éteignez le réseau chaque fois qu'il est pas utilisé.
- Éteignez le diffuseur d'identification du routeur, qui estfaçon dont l'appareil diffuse sa présence. Cela est inutile puisqueutilisateurs réels savent déjà qu'il existe.

Chapitre 8: Piratage un Smartphone

Ce chapitre couvrira la procédure que vous pouvez suivre pour pirater un smartphone Android. Vous devrez télécharger des logiciels spécialisés de tiers légitimes parties afin de rendre le processus plus facile et plus rapide.

Cette procédure est totalement anonyme et vous serez en mesure d'accéder à toutes les données dans le téléphone de la cible. Il est une exploitationdistance qui est effectuée via une connexion Internet sécurisée.

Étapes à suivre:

1. Allez sur le site MasterLocate*(MasterLocate.com)*pour utiliser l'applicationligne. Vous ne devez pas télécharger le logiciel sur votre ordinateur outéléphone pourutiliser. L'outil vous permettra de suivre la position GPS en temps réel de la cible,surveiller leurs SMS etmessages WhatsApp, écouter leurs appels etgarder trace de leur compte Facebook.
2. Exécutez l'application MasterLocate sur votre téléphone ou ordinateur.
3. Une boîte de dialogue devrait apparaître aveclasurterrain. *numéro mobile devictime*Entrez le numéro de la cible ici. Assurezque le téléphone de la cible estligne lorsque vous faites cette étape.
4. Dans la même boîtedialogue, justedessousla *Numéromobile devictime,* du champ il y a *Vérifier*. l'onglet Lorsque vous cliquez dessus, le programme tentera d'établir une connexion. Attendez que le pays de la cible à venir.
5. Une foisla connexion est établie et vérifiée, allez sur le côté droit de la boîte de dialogue. Parcourez la *Rapports* sectionpour affichermessages,journaux d'appels etfichiers de la cible. Si vous voulez télécharger quoice soit sur votre appareil, cliquez sur *Exporter Méthode.*Cela vous présentera des options pourformats de téléchargement, comme .zip et .rar.

Cette méthode de piratage smartphones est simple et direct. Toutvous devez faire estassurer que vous et la cible sontligne tout au long du

processus de piratage informatique. Toute interruption de la connexion Internet arrêtera le processus.autre chose est que vous devez connaître le numéro de téléphone de la victime ainsi que leur numérotéléphone mobile code pays.

Smartphone Hacking contremesures

Tant quetéléphone est connecté àréseau Wi-Fi non sécurisé ou contientlogiciels malveillants compromis, il est vulnérable àexploitation parpirates. Alorsquelles sont quelquesunes des mesures qui peuvent être prises pour obtenir un Smartphone contrepirates malveillants?

1. Assurezque votre téléphone estcoursexécutionun antivirus fiable, fiable et misjour.
2. Connecter uniquement pour sécuriserconnexion Wi-Fi lorsquenaviguez sur Internet,particulier danslieux publics.tels endroits sontmeilleurs terrain de chasse d'un pirate informatique pour avoir volédonnées des victimes sans méfiance. Wi-Fi publique ne doit pas être utilisé pouractivités qui nécessitent entrer vos coordonnées de compte bancaire, par exemple,achats ouservices bancaires.
3. Évitez la tendance à téléchargerapplications qui demandentaccès à vos renseignements personnels.
4. Assurezvous que tousfirmwares est constamment misjour, automatiquement ou manuellement.
5. Si vous avez des doutes quant à la source d'un logiciel,laisser seul. Seulement acheter ou télécharger des magasins d'applications vérifiées. Découvrez ce que les commentaires disent de mieux comprendre ce queautres quiont utilisé disent.
6. Verrouillez votre téléphonechaque fois que ce n'est pas utilisé. Assurezque votre motpasse fort et changer régulièrement.
7. Si vous recevezmessages texte contenantliens, ne cliquez pas sur le lien, surtout si vous ne connaissez pas l'expéditeur. Il est préférable de supprimer ces messages de spam dès qu'ils entrent dans votre téléphone.pirates informatiques ont tendance à envoyer des textes àmilliers d'utilisateurs de téléphones prétendant être des entreprises légitimes ousites Web. Lorsque le lien est cliqué, logiciel malveillant est installé sur le téléphone,permet ainsidonnées à accéder.

Il y amilliards de téléphones mobiles dans le monde entier, ceest une zone de piratage informatique qui offre le plus rapide etplus facile d'attaquer une cible.plupartgens ont tendance à se méfier quand ils sont sur leurs ordinateursmaisquelque sorte baisser leur garde

lorsnavigation sur leur téléphone. Il est donc extrêmement important quegens restent vigilants en tout temps.

Chapitre 9: Piratage Conseils pourdu débutant

Vousacheté ce livre parce que vous vouliez apprendre certaines des compétences fondamentales et techniques pourpiratage. Ne seraitil une honte si vous avez fini par se Busted, ou pire encore, piraté par un pirate informatique compagnon avec plusexpérience?

Il est très important que vous assurezvous que vous prenez soin extrême lorsdémarrage. Oui, il y a beaucoup de plaisir lorsque vous commencez à voir les résultats de votre travail, mais vous devez comprendre comment manœuvrer et nedétectés.

Voici cinq conseils clés que tousdébutants devraient suivre:

1. éviter le piège deachatlogicielspiratage de sites Webhasard. Il y amilliers d'arnaqueurs qui prétendent avoirlogiciels etoutils qui sont « garantis » au travail, mais ceuxci sont généralement misplace pour attirerpirates débutants. Vous perdrez votre argent en échange de logiciels inutiles. Vous pouvez même avoir vos propres données personnelles volées ainsi. Assurezvous que vous neaffaire avecsites Web légitimes ou vérifiés. Faites vos recherches bien et savoir ce queautres pirates utilisent et où ils les reçoivent de.
2. Évitez la tentation de télécharger freeware de l'Internet. Ceuxci comprennentpluparttemps keyloggers et chevauxTroie. Si vous êtes sérieuxsujetpiratage, vous devez être prêt à dépenserpeuargent pour obtenirchoses qui fonctionne. Le meilleur etplus efficacelogiciels est pas libre. Être un radin et aller pour les freebies vous exposer àpirates d'escroquerie malveillants qui ne manqueront pas d'exploiter votre système.
3. Lorsachatoutilspiratage, essayez d'utiliser Bitcoins. Il y a quelques outils que vous ne voulez pas faire remonter à vous, par exemple,serveurs privés virtuels, anonymes VPS et serveurs d'enregistrement de domaine. Si vous utilisez votre carte de crédit personnelle, vous pouvez vous exposer à plus d'un, et une vérification rapide de votre compte révélera vos activités de piratage. Le meilleur coup est de toujours garder votre véritable identité distincte de vos activitésligne.
4. Apprenez à développer vos compétences. Si vous êtes

qualifiés dansdéveloppement web seul, alors vous devrez apprendrepeuprogrammation. Si vous êtes un programmeur, puis apprendreécriture de script. L'objectif est de savoir quelque chosesujettout plutôt queobtenir l'aiseêtre dans une boîte.

5. Il est OK au début d'utiliser le logiciel d'autres personnes pour lancer vos attaques. Cependant, chaque pirate apprendvaleur son seltôt ou tard comment écrire ses propres codes, programmes et scripts. Si vous pouvez créer vos propres outils de piratage, alors vous aurez passé à l'étape suivante etdelà versêtre un hackerélite.

Conclusion

Nous sommes arrivés à la fin d'un long voyagetravers le monde du hacking. Si vous ne saviez pas quoice soit sur le sujet, alors vous devriez avoir suffisammentconnaissances maintenant pour commencerréaliserpetits exploits.

Il y a beaucoup de potentiel danspiratage, et ce ne sont pas tous malveillants. Apprendre à pirater est effectivement la meilleure façon de restersécurité dans un monde oùvérificationvotre email est dangereux, etparler à cet étranger mignon peut conduire à plus que ce que vous attendiez (et non pas une bonne façon)!

Que ce soit un appareil mobile ou un ordinateur de bureau,vigilance totale doit être maintenue. Les pirates sont toujours à l'affût, alors vous devez apprendre leurs trucs etcontrer.tant que guide de piratage éthique, ce livre vous a montré les premières étapes pourpiratage, ainsi quevous protéger.

Continuezapprendre et appliquer ce que vous avez appris ici. Rappelezvous de restersécurité en tout temps, et ne pas en dessusvotre tête.

Bonne chance!

Resources

www.csoonline.com

www.giac.org

www.whitehatsec.com

www.sans.org

www.2-spyware.com